



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/724,920	12/01/2003	Christophe Le-Rouzo	500200906-2	1841

7590 11/28/2007
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

ABEDIN, SHANTO

ART UNIT	PAPER NUMBER
----------	--------------

2136

MAIL DATE	DELIVERY MODE
-----------	---------------

11/28/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/724,920	Applicant(s) LE-ROUZO ET AL.	
	Examiner Shanto M Z Abedin	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 03 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 September 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2 and 4-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-2 and 4-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This is in response to the amendment filed on 09/19/2007.
2. Claims 1-2 and 4-21 are currently presented for the examination.
3. Claims 1-2 and 4-21 have been rejected.

Response to Arguments

4. Objection to DRAWINGS: The applicant's arguments regarding previous objection to the drawings are considered, and previous objection to the drawings are withdrawn.
5. Objection to TITLE: The title submitted on 09/19/2007 is accepted, and therefore, previous objection to the title is withdrawn.
6. Objection to ABSTRACT: The abstract submitted on 09/19/2007 is accepted, and therefore, previous objection to the abstract is withdrawn.
7. Objection to CLAIMS: The previous objection to claim 20 is withdrawn because of the amendments made to the claim.
8. Rejection under 35 USC 112: The applicant's arguments regarding the 35 USC 112 type rejections of claims 1-20 are found persuasive, therefore, the previous 35 USC 112 type rejections of claims 1-20 are withdrawn.
9. Rejection under 35 USC 101: The applicant's arguments regarding the 35 USC 101 type rejections of claims 1-11 and 15-17 are found persuasive, therefore, the previous 35 USC 101 type rejections of claims 1-11 and 15-17 are withdrawn.

Art Unit: 2136

10. Rejection under 35 USC 102 (b) : The applicant's arguments regarding the 35 USC 102 (b) type rejections of claims 1-20 are found persuasive, however, these arguments are now moot in view of new grounds of rejection presented in this office action (please see below for detail).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claims 1-2, 4-10 and 12-21 are rejected under 35 USC 103 (a) as being unpatentable over Hypponen et al (US 6577920 B1) in view of Kephart et al (US 5675711).

Regarding claim 1, Hypponen et al discloses a method of detecting a non-virus component in a virus-protected computer system having antivirus software comprising: identifying a software trace of the non-virus component (Col 2, starting at line 24; Col 3, starting at line 34; screening; identifying signature indicative of virus free macros; virus free macros are interpreted as non-virus software trace) and conveying the trace to the computer system as a virus pseudo-signature to allow detection of the component by the system's antivirus software (Col 2, starting at line 24; Col 5, starting at line 10; sending/ conveying macro signatures from network manager to user; scanning/ screening for virus

free macros) ; wherein the component is a hardware device (Col 2, starting at line 24; memory for storing signatures).

Hypponen et al fails to disclose wherein the software trace is indicative of the presence of the hardware device in the computer system.

However, Kephart et al discloses wherein the software trace is indicative of the presence of the hardware device in the computer system (Fig 4; Col 10, starts at line 20; determining 'pseudo' non-viral boot sector). Kephart et al further discloses identifying a software trace of the non-virus component and conveying the trace to the computer system as a virus pseudo-signature to allow detection of the component by the system's antivirus software (Col 8, starting at line 60; pseudo/ non-viral features).

Kephart et al and Hypponen et al are analogous art because they are from the same field of endeavor of virus signature system . At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teachings of Kephart et al with Hypponen et al to design a method further including wherein the (pseudo) software trace is indicative of the presence of the hardware device in the computer system in order to provide further hardware specific security.

Regarding claim 12, it is rejected applying as above rejecting claim 1, furthermore, Hypponen et al discloses a method of detecting, in a virus-protected computer system, the presence of a non-virus component comprising receiving a virus pseudo-signature associated

with a software trace of the non-virus component (Col 2, starting at line 24; Col 3, starting at line 34; screening; identifying signature indicative of virus free macros), and comparing the pseudo-signature with software traces disposed within the system's memory (Col 3, starting at line 34; determining).

Hypponen et al fails to disclose wherein the software trace is indicative of the presence of the hardware device in the computer system.

However, Kephart et al discloses wherein the software trace is indicative of the presence of the hardware device in the computer system (Fig 4; Col 10, starts at line 20; determining 'pseudo' non-viral boot sector). Kephart et al further discloses identifying a software trace of the non-virus component and conveying the trace to the computer system as a virus pseudo-signature to allow detection of the component by the system's antivirus software (Col 8, starting at line 60; pseudo/ non-viral features).

Regarding claim 14, it is rejected applying as above rejecting claim 1, furthermore, Hypponen et al discloses an apparatus for detecting, in a virus-protected computer system, a non-virus component, comprising a pseudo-signature generation element operative to produce a software trace of the component (Col 1, starting at line 65; Col 4, starting at line 50; signature/ checksum calculation), and an antivirus support source whereby the software trace may be conveyed, as a virus pseudo-signature, to the computer system (Col 2, starting

at line 24; Col 3, starting at line 34; screening; identifying signature indicative of virus free macros).

Hypponen et al fails to disclose wherein the software trace is indicative of the presence of the hardware device in the computer system.

However, Kephart et al discloses wherein the software trace is indicative of the presence of the hardware device in the computer system (Fig 4; Col 10, starts at line 20; determining 'pseudo' non-viral boot sector). Kephart et al further discloses identifying a software trace of the non-virus component and conveying the trace to the computer system as a virus pseudo-signature to allow detection of the component by the system's antivirus software (Col 8, starting at line 60; pseudo/ non-viral features).

Regarding claim 21, it is rejected applying as above rejecting claim 1, furthermore, Hypponen et al discloses a method of system of detecting a non-virus component in a virus-protected computer system having antivirus software comprising:

means for identifying a software trace indicative of the presence of a hardware device in the computer system; and

means for conveying the trace to the computer system as a virus pseudo-signature to allow detection of the device by the system's antivirus software (Col 2, starting at line 24; Col 3, starting at line 34),

wherein the trace is conveyed to the computer system as part of an update procedure (Col 2, starting at line 24; Col 5, starting at line 10),

whereby additional virus signatures or scanning engines may also be passed to the antivirus software (Col 2, starting at line 24; Col 5, starting at line 10).

Hypponen et al fails to disclose means for identifying a software trace indicative of the presence of a hardware device in the computer system.

However, Kephart et al discloses means for identifying a software trace indicative of the presence of a hardware device in the computer system (Fig 4; Col 10, starts at line 20; determining 'pseudo' non-viral boot sector).

Regarding claim 2, Hypponen et al discloses a method wherein the trace is conveyed to the computer system as part of an update procedure, whereby additional virus signatures or scanning engines may also be passed to the antivirus software (Col 2, starting at line 24; updating databases with macro signatures). Furthermore, Kephart et al discloses method wherein the trace is conveyed to the computer system as part of an update procedure, whereby additional virus signatures or scanning engines may also be passed to the antivirus software (Col 10, starts at line 20; plurality of pseudo viral features/ Vectors).

Regarding claim 4, Hypponen et al discloses a method wherein the software trace is resident in a volatile area of the system's memory (Col 3, starting at line 34; memory storing signatures indicative of virus free macros). Furthermore, Kephart et al discloses wherein the software trace is resident in a volatile area of the system's memory (Col 10, starts at line 20; boot sector).

Regarding claim 5, Hypponen et al discloses a method wherein the pseudo-signature is tagged or otherwise marked to distinguish it from authentic virus signatures (Col 3, starting at line 2; certified/ set of signatures indicative of virus free macros) . Furthermore, Kephart et al discloses wherein the pseudo-signature is tagged or otherwise marked to distinguish it from authentic virus signatures (Col 10, starts at line 20; classifier for pseudo non-viral, and viral features)

Regarding claim 6, Hypponen et al discloses a method wherein the antivirus software is modified so as to react differently to the presence of pseudo and authentic virus signatures (Col 1, starting at line 63; each micro having signature/ checksum).

Regarding claim 7, Hypponen et al discloses a method wherein the modification is effected as part of the update procedure (Col 2, starting at line 24; updating; macro signatures).

Regarding claim 8, Hypponen et al discloses a method wherein the antivirus software does not attempt to fix, clean, modify or delete the component associated with the pseudo-signature (Col 5, starting at line 15; only manager has authority to modify signature database).

Regarding claim 9, Hypponen et al discloses a method wherein detection of the pseudo-signature causes an advisory message to be conveyed to a user of the system, advising the user of the presence of the detected component (Col 3, starting at line 23; alerting).

Regarding claim 10, Hypponen et al discloses a method wherein detection of the pseudo-signature effects a connection to a website providing details of the component concerned (Col 3, starting at line 1; central site).

Regarding claim 13, Hypponen et al discloses a method wherein, in the event of a match being found, the antivirus software of the system is operative to convey, to a user of the system, an advisory message advising of the presence of the detected non-virus component (Col 3, starting at line 23; alerting).

Regarding claims 15 and 18, they recite the limitations of claims 1-2 and 4-14, therefore, they are rejected applying as above rejecting claims 1-2 and 4-14.

Regarding claims 16-17 and 19-20, they recite the limitations of claims 1-2, 5-6 and 12, therefore, they are rejected applying as above rejecting claims 1-2, 5-6 and 12.

12. Claim 11 is rejected under 35 USC 103 (a) as being unpatentable over Hypponen et al (US 6577920 B1) in view of Kephart et al (US 5675711) further in view of Muttik et al (US 6963978 B1).

Regarding claim 11, Hypponen et al discloses a method of facilitating the detection of a non-virus component in a first virus-protected computer system comprising: identifying, on a second computer system, a software trace of the non-virus the component (Col 2, starting at line 47; Col 4, line 50 to Col 5, line 22; network manager, or controller scanning or sending virus signatures to host/ end user application), and conveying the trace towards an antivirus update source whereby the software trace may be passed, as a virus pseudo-signature, to the first computer system (Col 2, starting at line 24; updating databases with macro signatures; relaying to the end user computer signature indicative of virus free macros); wherein the component is a hardware device (Col 2, starting at line 24; memory for storing signatures).

Hypponen et al fails to disclose wherein the software trace is indicative of the presence of the hardware device in the computer system.

However, Kephart et al discloses wherein the software trace is indicative of the presence of the hardware device in the computer system (Fig 4; Col 10, starts at line 20; determining 'pseudo' non-viral boot sector). Kephart et al further discloses identifying a software trace of the non-virus component and conveying the trace to the computer system as a virus pseudo-signature to allow detection of the component by the system's antivirus software (Col 8, starting at line 60; pseudo/ non-viral features).

In the case, grounds for the inherency of first and second computer system are found not to be supportable, Muttik et al discloses identifying, on a second computer system, a software trace of the non-virus the component and conveying the trace towards an antivirus update source whereby the software trace may be passed, as a virus pseudo-signature, to the first computer system (Fig 3-6; Col 6, line 1 -Col 8, line 67; transmitting fingerprinting of innocent data; client-server environment).

Müttik et al , Kephart et al and Hypponen et al are analogous art because they are from the same field of endeavor of virus signature system . At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teachings of Kephart et al and/ or Muttik et al with Hypponen et al to design a method further including wherein identifying, on a second computer system, a software trace of the non-virus the component and conveying the trace towards an antivirus update source whereby the software trace may be passed, as a virus pseudo-signature, to the first computer system in order to facilitate network antivirus updating.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in **ABANDONMENT** of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551, and fax number is 571-273-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. For more

Art Unit: 2136

information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

11/26/07